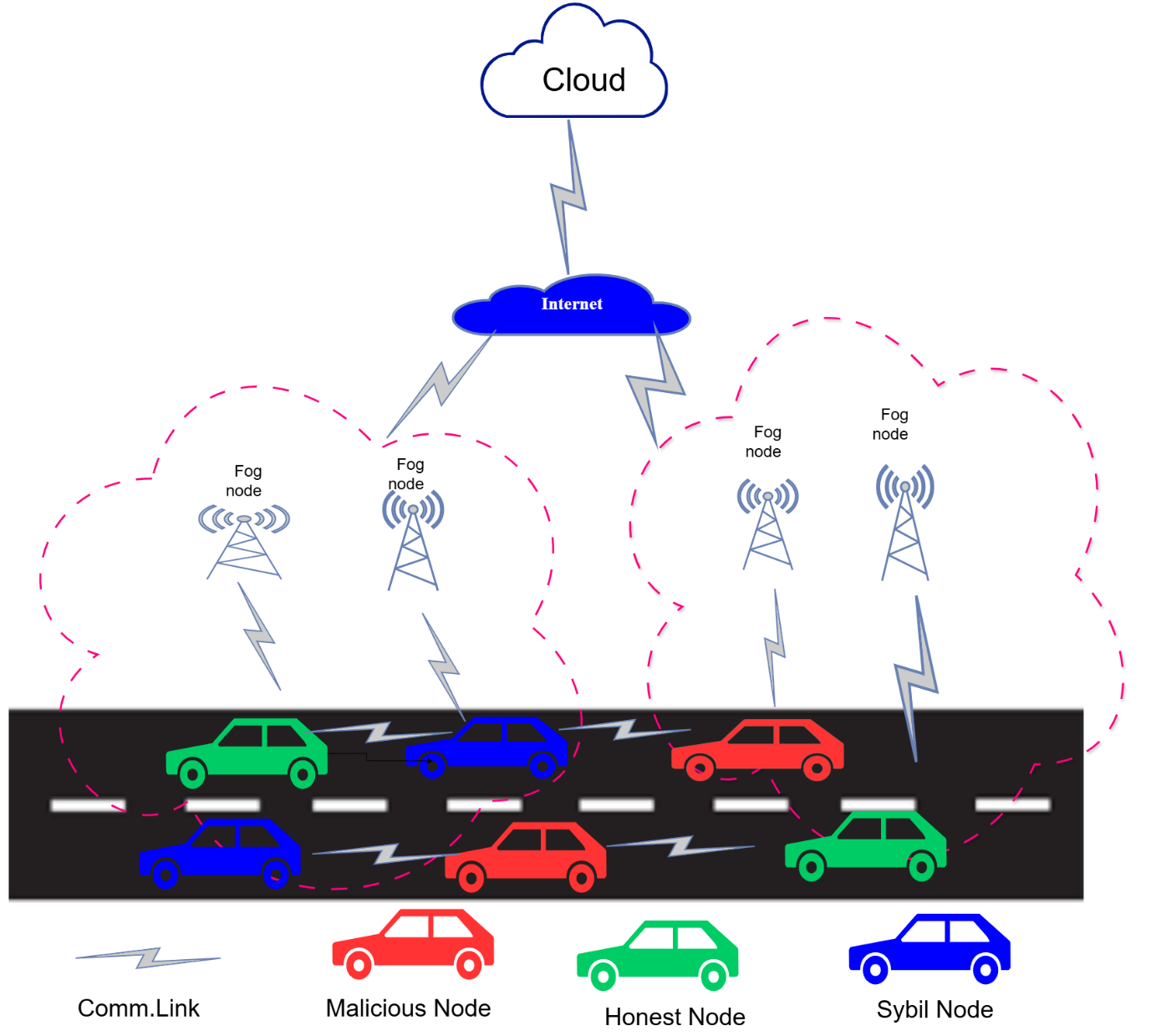
System architecture :



**Workflow :**

Below is a conceptual workflow illustrating how a Verifiable Delay Function (VDF) combined with a fog/cloud hierarchical architecture can be used to detect Sybil attacks in Vehicular Ad Hoc Networks (VANETs). This workflow assumes a layered infrastructure comprising on-vehicle units, Road Side Units (RSUs), fog nodes, and cloud servers, as well as an authentication and cryptographic framework that leverages VDFs.

**Key Components and Concepts**

* **VANET Environment:** Vehicles communicate wirelessly with one another and with infrastructure units (RSUs).
* **Sybil Attack:** A malicious vehicle forges multiple fake identities to gain unfair advantages (e.g., manipulating traffic information, influencing routing, or voting-based mechanisms).
* **Verifiable Delay Function (VDF):** A cryptographic primitive that requires a prescribed, non-parallelizable amount of computation time to produce a proof. The proof can then be verified quickly. Using VDFs discourages attackers from rapidly generating multiple valid identities in short intervals.
* **Fog Layer:** Intermediate computation/analysis nodes located at or near the RSUs. They provide lower-latency data processing, filtering, and preliminary detection steps before sending results to the cloud.
* **Cloud Layer:** A centralized (or regionally distributed) server infrastructure that aggregates global context, performs heavier analytics, stores historical data, and correlates suspicious patterns observed by multiple fog nodes.

**Step-by-Step Workflow**

1. **Initial Vehicle Registration and Credential Distribution:**
   * Each legitimate vehicle is provisioned with cryptographic credentials (public/private keys, certificates) from a trusted authority (such as a transportation authority or a PKI-based system).
   * Vehicles receive software that can compute and verify VDFs. These credentials and capabilities ensure that every legitimate identity can generate valid proofs over time.
2. **Normal Operation and Message Broadcasting:**
   * As vehicles move, they periodically broadcast beacons containing location, speed, direction, and identity information.
   * Each beacon includes:
     + Vehicle’s authenticated identity (or pseudonym/certificate).
     + A recent VDF output that proves that the vehicle spent a certain minimal and continuous amount of time deriving it.
     + A timestamp and possibly a cryptographic signature to ensure message integrity.
3. **Local Verification at RSUs / Fog Nodes:**
   * Road Side Units (RSUs) or dedicated fog nodes deployed close to the roadway continuously receive beacons from nearby vehicles.
   * The fog node checks:  
     **(a)** **Authenticity & Integrity:** Verifies signatures and certificates.  
     **(b)** **VDF Proof Verification:** Using a fast verifier algorithm, confirms that the VDF proof in the beacon is valid and that it corresponds to a genuine sequence of operations performed over the required time interval.
   * If a beacon lacks a valid VDF or uses an outdated certificate, it is immediately flagged as suspicious.
4. **Time-Windowed Observation and Identity Correlation at the Fog Layer:**
   * The fog node maintains a rolling time-windowed database of all recently observed vehicle identities and their corresponding VDF proofs and spatiotemporal data.
   * It looks for patterns indicative of Sybil attacks, such as:
     + **Spatial-Temporal Overlaps:** Multiple identities claiming to be at different nearby locations but derived from suspiciously similar VDF seeds or seen emerging at the same time.
     + **Infeasible Mobility Patterns:** Different identities purportedly controlled by the same attacker may attempt to appear as if they are traveling on distinct paths, but subtle timing or VDF inconsistencies can reveal the ruse.
   * The fog node can compute a preliminary Sybil suspicion score. If the same computational source (as evidenced by VDF correlation or identical time offsets) is producing multiple valid identities too frequently, suspicion arises.
5. **Local Mitigation and Reporting to the Cloud:**
   * If the fog node strongly suspects a Sybil attack, it can implement immediate local mitigation steps:
     + Temporarily filter or deprioritize messages from the suspicious identities.
   * The fog node then forwards a detailed report (including suspicious IDs, relevant VDF proofs, observed patterns) to the cloud layer for a global perspective.
6. **Global Analysis at the Cloud Layer:**
   * The cloud aggregates reports from multiple fog nodes spread across the region.
   * Correlation algorithms run at scale:
     + Cross-check suspicious identities across different geographic areas.
     + Identify patterns of VDF usage anomalies, such as the same computational artifacts or seeds appearing in multiple distant locations at nearly the same time (which is improbable for honest vehicles).
   * The cloud can also rely on historical data to see if these suspicious identifiers repeatedly show up or maintain improbable travel patterns over long ranges.

7. **Decision and Response Distribution:**

* Once the cloud has high-confidence evidence that certain identities are part of a Sybil attack, it can:
  + Revoke their certificates through a Certificate Revocation List (CRL) update.
  + Notify all fog nodes and RSUs to blacklist the identified malicious identities.
* Updates are propagated to the VANET infrastructure. Vehicles and RSUs will refuse to accept or forward messages from the revoked identities.

8. **Continuous Improvement and Adaptation:**

* The system continuously updates its detection models and thresholds based on observed attacker strategies.
* Cloud-level intelligence refines the VDF difficulty parameters or identity distribution policies to stay ahead of more sophisticated attackers.